

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

IN THE MATTER OF THE SEARCH OF INFORMATION
ASSOCIATED WITH THE CELLULAR DEVICE ASSIGNED
WITH 845-380-6209, THAT IS IN THE CUSTODY OR
CONTROL OF VERIZON WIRELESS

Case No.

2:21-MJ-153

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the _____ District of _____ New Jersey _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

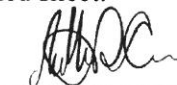
Code Section	Offense Description
18 U.S.C. § 1029	Access Device Fraud
18 U.S.C. § 1030	Computer Intrusion

The application is based on these facts:

See attached Affidavit.

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Anthony DeCicco, FBI Special Agent

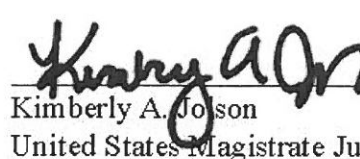
Printed name and title

Sworn to before me and signed in my presence.

Date: ~~03/01/2021~~

March 2, 2021

City and state: Columbus, OH 43215


Kimberly A. Johnson
United States Magistrate Judge



IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
CELLULAR DEVICE ASSIGNED WITH
845-380-6209, THAT IS IN THE CUSTODY
OR CONTROL OF VERIZON WIRELESS

Case No. _____

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Anthony DeCicco, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain cellular device assigned with number **845-380-6209** (“the SUBJECT ACCOUNT”), with listed subscriber(s) **Christopher BJORK**, father to **Cory BJORK** or that is in the custody or control of **Verizon Wireless**, a wireless communications service provider that is headquartered at **180 Washington Valley Road, Bedminster, NJ 07921**. As a provider of wireless communications service, **Verizon Wireless** is a provider of an electronic communications service, as defined in 18 U.S.C. § 2510(15).

2. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) and Federal Rule of Criminal Procedure 41 to require Verizon Wireless to disclose to the government the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

3. Because this warrant seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information

collected by a “pen register” and/or “trap and trace device,” *see* 18 U.S.C. § 3127(3) & (4), the requested warrant is designed to also comply with the Pen Register Act. *See* 18 U.S.C. §§ 3121-3127. The requested warrant therefore includes all the information required to be included in an order pursuant to that statute. *See* 18 U.S.C. § 3123(b)(1).

4. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been since October 2019. I am currently assigned to the Cincinnati Field Office, Columbus Resident Agency, Cyber Crime Squad, which is responsible for investigating computer and high-technology crimes. During my career as an FBI SA, I have participated in numerous cyber-related investigations. During the investigation of these cases, I have participated in the execution of numerous arrests, search warrants, and seizures of evidence. Since my assignment to the Cyber Crime Squad, I have received both formal and informal training from the FBI regarding cyber investigations. I am trained and authorized to investigate the offenses alleged herein. Prior to working with the FBI, I received a Master of Science in Computer Information Systems and cyber security from Boston University and I am certified through the SANS Institute GIAC Security Essentials (GSEC) course.

5. The facts in this affidavit come from my personal observations, my training and experience, my review of documents, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1029 (access device fraud) and 18 U.S.C. § 1030 (computer intrusion) have been committed by Cory BJORK, and as-yet unidentified co-conspirators. There is also

probable cause to search the information described in Attachment A for evidence of these crimes as further described in Attachment B.

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

8. In or around April 2020, the FBI received information from LBrands (the VICTIM) detailing a compromise of the reward points system of Bath & Body Works (BBW), a subsidiary of the VICTIM. Among the information provided was a forensic report which included: (a) a list of reward points obtained without authorization from the BBW reward system; (b) logs of IP addresses used to make millions of requests to the BBW reward points system; (c) a summary of Discord communications; and (d) open source research pointing to two individuals, Cory BJORK and Panagiotis KALOGEROPOULOS, for disseminating the reward points from the BBW reward points system.

9. Based on an interview with Mark STORTS, Asset Protection Manager for the VICTIM, in or around September 2019, BBW initiated a loyalty rewards program in select regions. Between approximately October 2019 and January 2020, an unknown individual, or individuals (“the SUBJECT”) gained unauthorized access to the VICTIM’s online reward points system, via a vulnerability in the BBW website. The vulnerability was due to the reward points being stored in plaintext versus ciphertext. The SUBJECT was able to acquire the plaintext reward points, and then sell or redeem the reward points.

10. The SUBJECT utilized different social media platforms, to include the Discord accounts listed above, to sell the reward points acquired through unauthorized access of the VICTIM's online reward points system. For example, based on the VICTIM's analysis, the Discord accounts "Clout#1111", "Corybusiness#1667", and "CloutCobain#0001" were found on the websites hackforums.net and nulled.to, selling the reward points. According to the VICTIM, an estimated loss of approximately \$760,000, a dollar amount based on the estimated value the VICTIM places on each reward point, was incurred.

11. According to open source research, hackforums.net and nulled.to are internet-based websites that can be found using a normal web browser. The Wikipedia article on Hack Forums describes the website as an internet forum that has been widely reported as facilitating criminal activity. Similarly, the Wikipedia article on Nulled describes the website as an online forum board used by cyber criminals.

12. The forensic report, provided by the VICTIM, included a summary of Discord communications between the user Clout#1111 and an employee with Intel471, a remediation company hired by the VICTIM, who posed as a buyer. The Intel471 employee made a controlled purchase of approximately 200 reward points from Clout#1111. The approximate 200 reward points were confirmed to be stolen from BBW's website by cross-referencing BBW logs.

13. As part of the Discord communications with the Intel471's employee, user Clout#1111 admitted to gaining access to the BBW rewards point system by exploiting a vulnerability in the BBW website, the same vulnerability mentioned above. User Clout#1111 also offered to sell the method of gaining unauthorized access to the BBW reward points system for €150. Furthermore, Clout#1111 claimed to be the individual to find the vulnerability in the

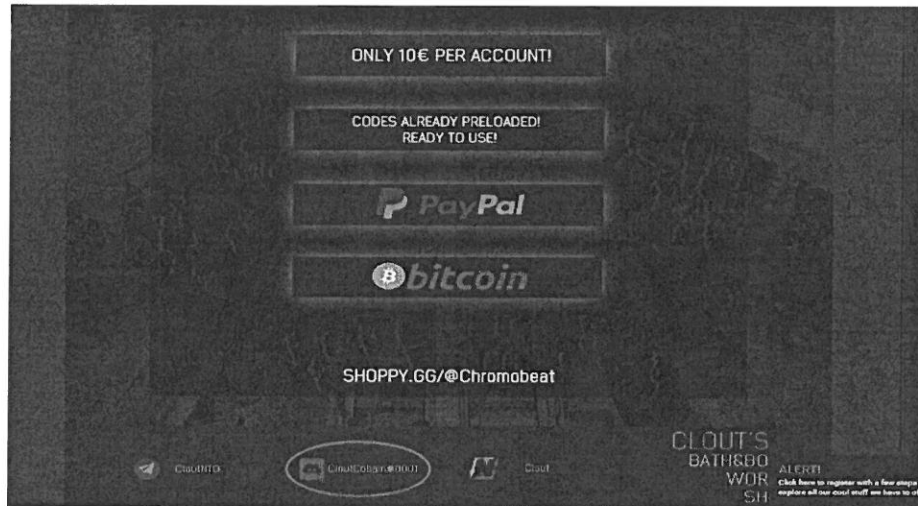
BBW loyalty rewards system and claimed to earn €35+ a day selling BBW reward points over the past two months.

14. In or around May 2020, a screenshot taken of the website nullled.to revealed Clout#1111 posted an advertisement for the sale of BBW reward points. The advertisement contained a link to the Discord Server: <http://discord.gg/Bg3RVjQ> and listed the point of contact for the exchange as Clout#1111, see screenshot below. Based on my training and experience, Discord servers are used to facilitate group chats. A Discord server is used to delineate different discussions. For example, if someone has a Discord server for a video game, a user who joined the server can join different discussion threads such as one labeled “#General” or another discussion thread named “#Trades.” In this context, the discussion threads could be used to host the exchange of different illicit material.

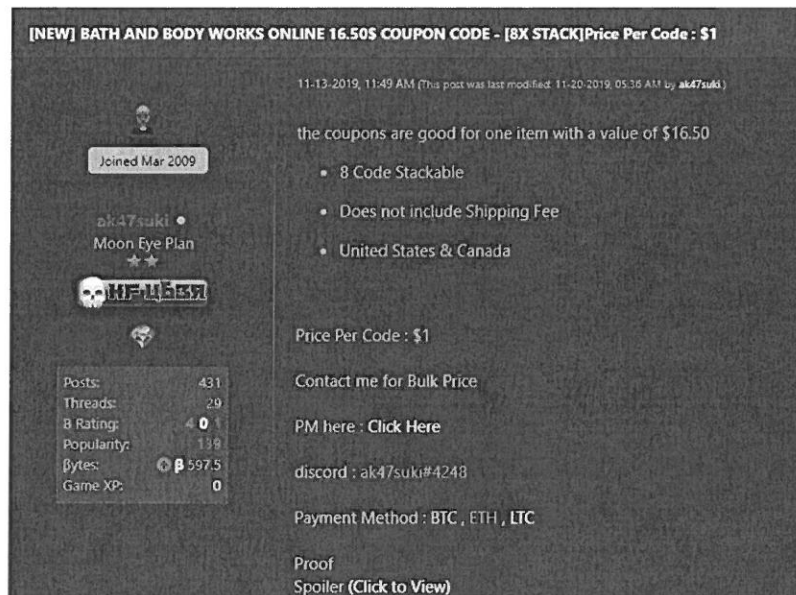


15. In or around May 2020, open source research was conducted and revealed user Clout#1111 also utilized the Discord account Cloutcobain#0001, as seen on an advertisement for

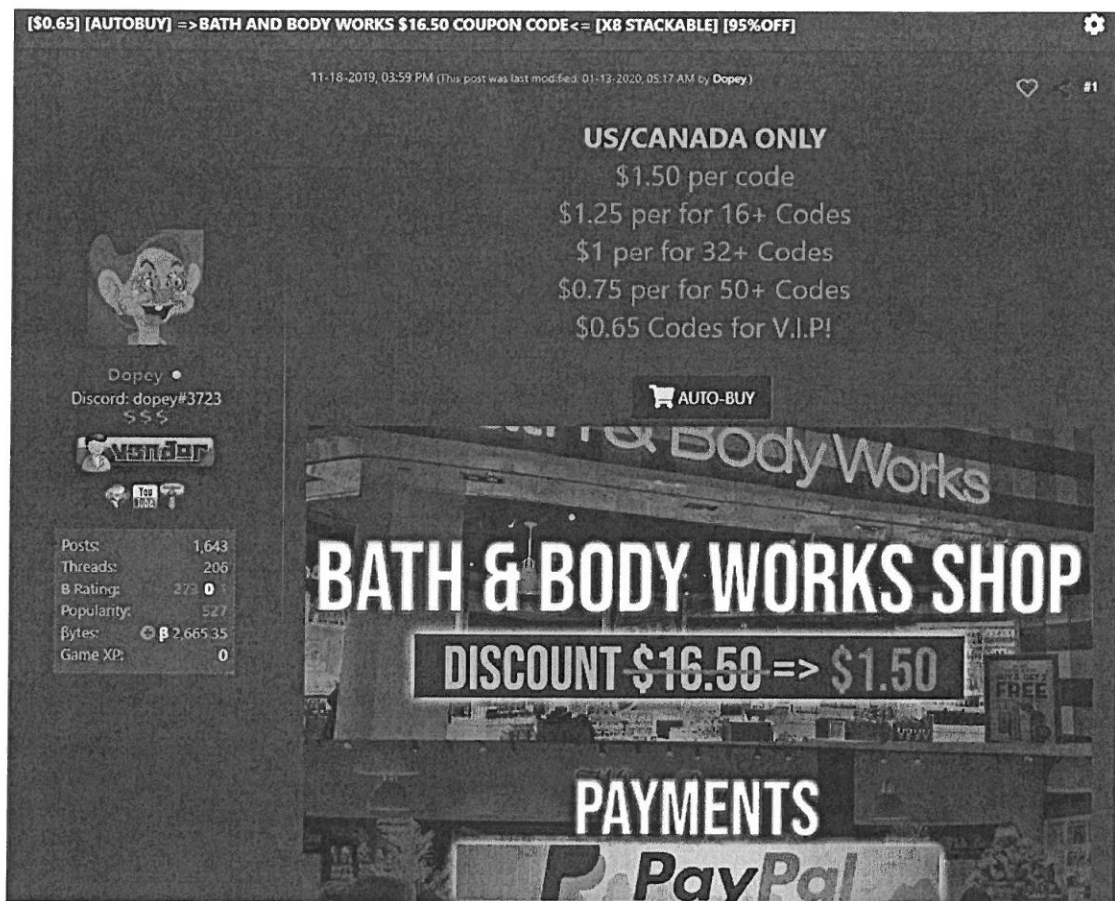
BBW reward points on the website nulled.to, see screenshot below. Based on the hackforums.net and nulled.to posts, the Discord accounts are used to negotiate terms of sale of the BBW reward points.



16. In or around May 2020, a screenshot taken of the website hackforums.net revealed user AK47suki posted an advertisement for the sale of BBW reward points, in or around November 2019. The price listed for each code was \$1.00 and the method of communication for the exchange was listed as Discord account AK47suki#4248, see screenshot below.



17. In or around May 2020, a screenshot taken of the website hackforums.net revealed user “Dopey” posted an advertisement for the sale of BBW reward points, in or around November 2019. The price listed for each code was \$1.50, or \$0.75 for bulk orders of 50 or more. The method of communication was listed as Discord account Dopey#3723, see screenshot below.

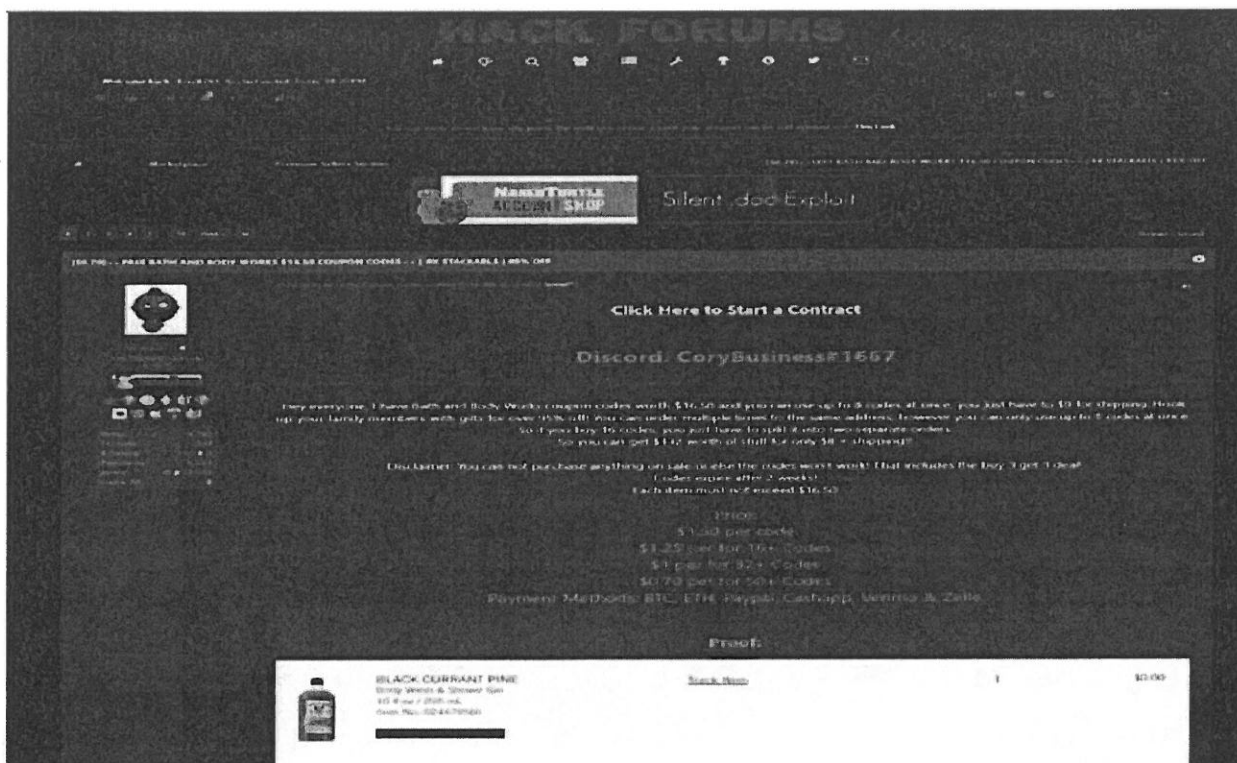


18. In or around May 2020, screenshots taken of the website hackforums.net and Google revealed that, in or around November 2019, a user named “Stoned” created a thread that advertised the sale of BBW reward points. The thread listed the price per code as \$1.50, or less if purchased in bulk. Methods of payments were listed as Bitcoin, Ethereum, PayPal, Cashapp, Venmo, and Zelle. The thread also listed the Discord account CoryBusiness#1667 as the main method to negotiate transactions. See screenshots below.

hackforums.net › Profile of Who is Tony

Profile of Who is Tony - Hack Forums

Nov 13, 2019 - Discord: **CoryBusiness#1667**. Hey everyone, I have Bath and Body Works coupon codes worth \$16.50 and you can use up to 8 codes at once, ...



19. In or around June 2020, Discord provided results to the FBI for account information linked to Clout#1111. Results showed multiple logins from Internet Protocol (IP) address 77.49.243.253, verified associated email as panman101mw3@yahoo.com, and phone number +306944232445.

20. Open source tools were used to determine the Internet Service Provider for the IP address 77.49.243.253. The results resolved to Internet Service Provider (ISP) FORTHnet SA, a Greek ISP.

21. In or around July 2020, Facebook provided results to the FBI for account Panagoitis Kalogeropoulos. Results showed multiple IP logins from FORTHnet SA ISP, phone number +306944232445, email address panman101mw3@yahoo.com, and phone model OnePlus A6003.

22. According to the BBW reward system IP logs, IPs tied to the fraudulent orders placed on December 31, 2019 were: 209.58.148.156, 108.255.199.58, 99.228.251.9, and 100.40.199.167. Based on open source research, the first three IP addresses return to a proxy, however, IP address 100.40.199.167 resolves to ISP Verizon FIOS from Poughkeepsie, NY.

23. According to the VICTIM forensic report, user CoryBusiness#1667 created nulled.to account “Stoned” using IP address 100.40.212.140. Shortly after the IP address 100.40.199.167 was captured on December 31, 2019, “Stoned” posted a screenshot of a BBW purchase they made on nulled.to as proof that the exploit was working.

24. According to the forensic report conducted by the VICTIM, IP addresses on network 100.40.* return to ISP Verizon FIOS in Poughkeepsie, NY. In or around September 2020, open source research was conducted to show the IP range associated with Verizon FIOS. Results showed Verizon FIOS is assigned Autonomous System Number (ASN) 701. Further research revealed ASN 701 owns IP Range 100.40.0.0/17. Therefore, IP addresses 100.40.212.140 and 100.40.199.167, as mentioned above, fall within Verizon FIOS’s network.

25. In or around June 2020, Discord provided results to the FBI for account information linked to CoryBusiness#1667. Results showed approximately 1,405 logins from IP addresses 100.40.181.48 and 100.40.212.140, phone number +18453806209, with a verified associated email as cory.BJORK4@gmail.com. Results also showed 2,112 logins from IP address 75.183.110.195 and 75.183.104.226.

26. Open source tools were used to determine the Internet Service Provider for IP addresses 75.183.110.195 and 75.183.104.226. The results resolved to Spectrum in Burlington, North Carolina.

27. In or around July 2020, Instagram provided results for account information Cory BJORK. Results revealed a creation IP address of 100.40.212.140, phone number +18453806209, and email address corybusiness@outlook.com.

28. Open source tools were used to determine the Internet Service Provider for the IP addresses 100.40.181.48 and 100.40.212.140. The results resolved to Verizon FIOS.

29. In or around July 2020, Verizon FIOS provided results to the FBI for account information linked to the IP addresses 100.40.212.140 and phone number +18453806209. Results showed customer name as Christopher BJORK, account address 27 Walnut Hill Road, Poughkeepsie, NY 12603, phone number +18454377841, and email address walnuthillrd@yahoo.com. Open source research indicated Christopher BJORK was father to the subject Cory BJORK.

30. Based on my training and experience, I know that wireless providers such as Verizon Wireless typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless communication service. I also know that wireless providers such as Verizon Wireless typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular device and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the SUBJECT ACCOUNT's user or users and may assist in the identification of co-conspirators and/or victims.

AUTHORIZATION REQUEST

31. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41. The proposed warrant will also function as a pen register order under 18 U.S.C. § 3123 authorizing the installation and use of a pen register and/or trap and trace device to record, decode, and/or capture certain information in Attachment A for each communication to or from the SUBJECT ACCOUNT, without geographic limit, for a period of forty-five days (45) days pursuant to 18 U.S.C. § 3123(c)(1).

32. I further request that the Court direct Verizon Wireless to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on Verizon Wireless who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

33. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation, including by giving targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.

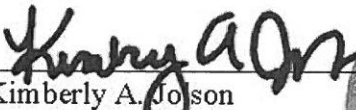
Respectfully submitted,



Anthony DeCicco
Special Agent
Federal Bureau of Investigation

March 2, 2021

Subscribed and sworn to before me on ~~March~~ ~~1st~~, 2021


Kimberly A. Johnson
United States Magistrate Judge



ATTACHMENT A

Property to Be Searched

This warrant applies to records and information associated with the cellular device assigned **VOL Account Number: 0139147030141, MSIN +18453806209** (“the SUBJECT ACCOUNT”), with listed subscriber **Christopher BJORK**, father of **Cory BJORK** (“the SUBJECT”), that is in the custody or control of **Verizon Wireless**, a wireless communications service provider that is headquartered at **180 Washington Valley Road, Bedminster, NJ 07921**.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A:

- a. The following information about the customers or subscribers associated with the SUBJECT ACCOUNT for the time period **October 1, 2019 to date of this warrant**:
 - i. Names (including subscriber names, user names, and screen names);
 - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
 - iii. Local and long distance telephone connection records;
 - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
 - v. Length of service (including start date) and types of service utilized;
 - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");
 - vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
 - viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

ix. For the period of **October 1, 2019 to the date of this warrant**, all records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the SUBJECT ACCOUNT, including:

(A) the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

(B) information regarding the cell tower and antenna face (also known as “sectors” through which the communications were sent and received), as well as Network Event Location System data (also known as “NELOS”).

b. Information associated with each communication to and from the SUBJECT ACCOUNT for a period of **45 days from the date of this warrant**, including:

- i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;
- ii. Source and destination telephone numbers;
- iii. Date, time, and duration of communication; and
- iv. All data about the cell towers (i.e. antenna towers covering specific geographic areas) and sectors (i.e. faces of the towers) to which the SUBJECT PHONE will connect at the beginning and end of each communication as well as Network Event Location System data (also known as “NELOS”).

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence and instrumentalities of violations of 18 U.S.C. § 1029 (access device fraud) and 18 U.S.C. § 1030

(computer intrusion) involving **Cory Bjojr** during the period **October 2019 to the date of this warrant.**

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS
PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by VERIZON WIRELESS, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of VERIZON WIRELESS. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of VERIZON WIRELESS, and they were made by VERIZON WIRELESS as a regular practice; and
- b. such records were generated by VERIZON WIRELESS electronic process or system that produces an accurate result, to wit:
 1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of VERIZON WIRELESS in a manner to ensure that they are true duplicates of the original records; and
 2. the process or system is regularly verified by VERIZON WIRELESS, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature